THE CUBICLE CULPRITS

cyberhaven

Insider Risk Report

Q1 2024

THE CUBICLE CULPRITS

Table of contents

01 Key findings

02 Methodology

03 What sensitive data is exfiltrated

04 Remote, hybrid, and office work arrangements

05 How employees exfiltrate sensitive data

06 Anatomy of a layoff

Introduction

In today's business environment, company leaders are increasingly vigilant about the security of their data, especially as work arrangements evolve. With the rise of remote and hybrid work, there's been a prevailing belief that employees outside the office are more likely to misuse company data. However, our latest research suggests the situation is more nuanced.

This report investigates insider risks associated with different work environments: in-office, remote, and hybrid. It also considers how organizational changes, such as layoffs, may influence the likelihood of data theft. In contrast to previous assumptions, our analysis reveals that it's often the in-office employees who present a greater risk, particularly when they're working away from their usual environment.

> “HYBRID AND REMOTE WORK REQUIRES DATA AVAILABILITY OUTSIDE TRADITIONAL OPERATING ENVIRONMENTS, WHICH IN TURN COMPLICATES DATA PROTECTION.”
>
> Gartner

Our approach is detailed and data-driven. What makes this report unique is that unlike surveys that ask IT security professionals what they think is happening, we've analyzed the behavior of over 3 million workers, precisely tracking how they handle sensitive information. The insights we offer are surprising and vital: the data at risk is often customer data or the most valuable IP.

This report presents these findings and sheds light on the intricate patterns of data movement within organizations. We provide this information with the goal of equipping businesses with the knowledge to better protect their data. Understanding the real dynamics of insider risks is the first step in preventing potential data security incidents.

And these days, where employees work is a critical factor for the risk to company data.

Key findings

01 REMOTE AND HYBRID WORKPLACE ARRANGEMENTS

Counterintuitively, **office-based workers are 77% more likely** than their remote counterparts to exfiltrate sensitive data.

But when office-based workers login from offsite, they are **510% more likely** to exfiltrate data than when onsite at the office, making it the riskiest time for corporate data.

02 IMPACT OF A LAYOFF ON DATA EXFILTRATION

In the 24 hours before employees are terminated in a layoff, we found a **720% increase in data exfiltration** compared to the baseline.

The first measurable increase in data exfiltration begins **200 days before a layoff,** and by three weeks before a layoff data exfiltration reaches **150% of baseline.**

03 WHAT TYPES OF DATA EMPLOYEES EXFILTRATE

Overall, the most common sensitive data employees exfiltrate are client and customer data **(31.2% of data by volume)** and source code **(16.5%).**

The week before a layoff, workers are more likely to take source code **(348% increase),** design files and formulas **(769% increase),** and sensitive project files **(440% increase).**

04 HOW SENSITIVE DATA LEAVES THE COMPANY

The most common exfiltration vectors are personal cloud storage **(22.7% of incidents),** removable media **(15.6%),** generative AI tools **(13.1%).**

When employees are offsite, the way data leaves changes. Offsite, data exfiltration via Bluetooth/AirDrop is **400% more likely** and removable storage is **254% more likely.**

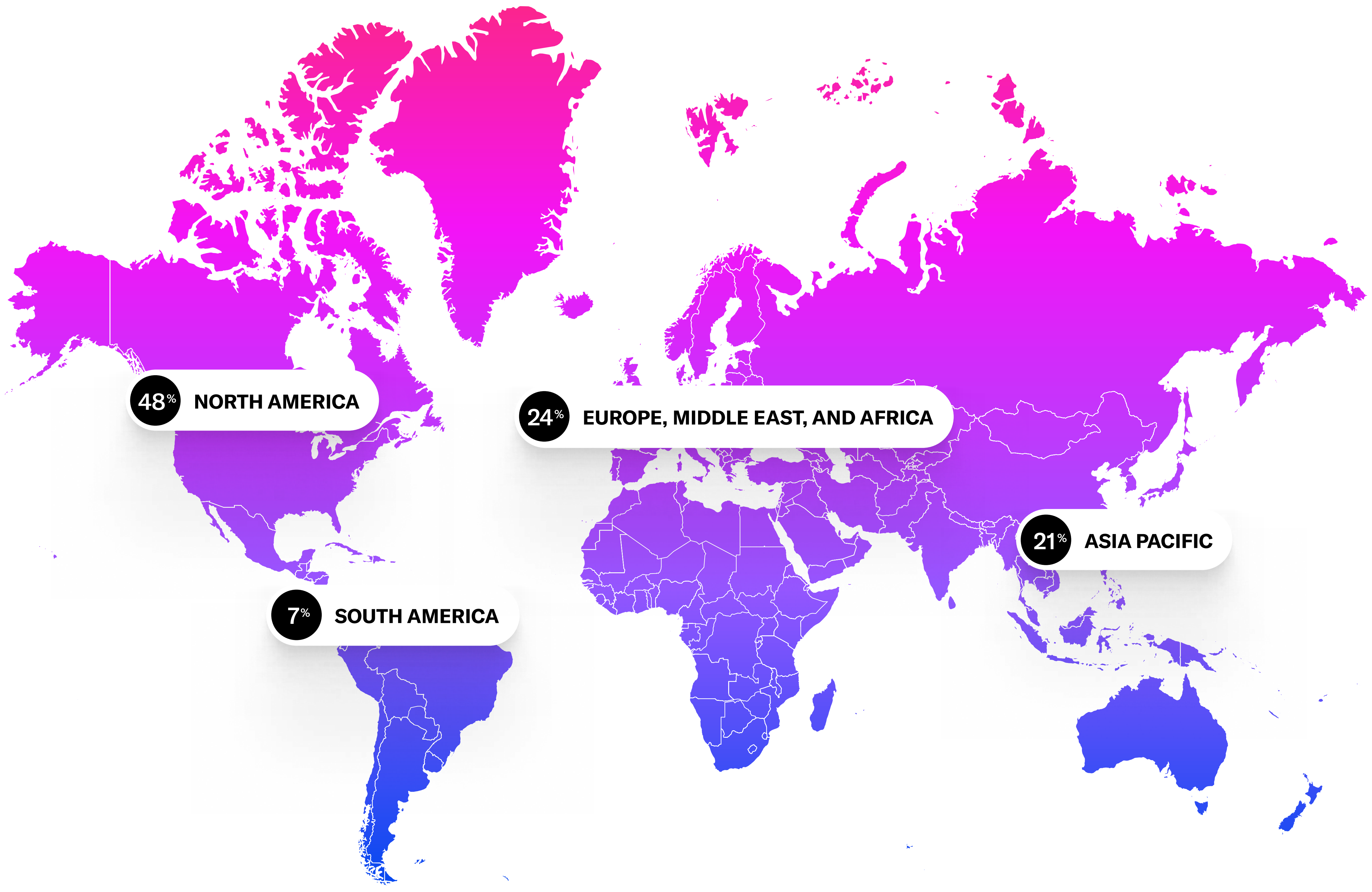
Methodology

To compile the findings in this report, we analyzed 831,000 data exfiltration incidents and anonymized usage data for over 3 million workers from November 1, 2023 to January 31, 2024 using the Cyberhaven product. The companies in our sample represent 13% of the Fortune 100 and span multiple industries.

Top industries represented in the report

Biotech and pharma	8%
Chemicals	3%
Engineering	4%
Financial services	18%
Healthcare	16%
Legal	5%
Manufacturing	14%
Technology	21%

Geographic distribution in our sample



HOW WE CLASSIFIED DATA AS SENSITIVE

We use multiple signals to determine whether a piece of data is sensitive. The content of the data is important, but equally important is where the data originated, how it was handled, and who interacted with it throughout its journey in the company. For example, we classify information like names and phone numbers originating in a company's data warehouse for customer data as customer data, even after it leaves that repository. But we don't classify names and phone numbers that originate on an external, public website as sensitive.

HOW WE DEFINE AN INCIDENT

In multiple sections of this report we discuss the number of data exfiltration incidents. Data exfiltration, simply put, is transferring data outside the organization in unapproved ways. Exfiltrating sensitive data is risky, but it doesn't always turn into an insider threat. And not all insider threats are intentional or malicious, either. For example, employees sometimes email sensitive information to the wrong person outside the company by mistake, or they copy a sensitive document to a USB drive to work on it at home, only to lose the drive and its data.

What sensitive data is exfiltrated

The top 10 types of sensitive data employees exfiltrate includes:

1 **CLIENT/CUSTOMER DATA**

Example: a spreadsheet exported from NetSuite showing all customers and the dollar amount they've paid over the past year, an M&A plan that a publicly traded client of an investment bank shared with the bank's deal team, etc.

2 **SOURCE CODE**

Example: the code used in a social media app to determine what content to show a user in their feed, the algorithm a buy-now-pay-later company uses to determine whether to extend credit to a customer at checkout, etc.

3 **REGULATED PERSONAL DATA (PII)**

Example: a California customer's name and mailing address stored by an e-commerce company as part of their order tracking system, a German user's date of birth stored by a social media company, etc.

4 **DESIGN FILES AND PRODUCT FORMULAS**

Example: a 3D CAD file with the parts and assembly of a LiDAR sensor package for a self-driving car in development, the recipe and production process for a popular candy bar, etc.

5 **SENSITIVE PROJECT FILES**

Example: a folder of images taken with the unannounced smartphone that could be analyzed to reveal specifications of the new camera, an unreleased movie stored on a share drive by a production house that makes movie trailers, etc.

6 **REGULATED FINANCIAL DATA (PCI)**

Example: a customer's credit card number stored in a billing application for a water utility in order to process recurring payments, a folder with new customer signup forms containing bank account and routing numbers, etc.

7 **REGULATED HEALTH DATA (PHI)**

Example: the medical record of a celebrity who was checked into the hospital following a serious car accident, a CSV file downloaded from an insurance billing application containing patient names and diagnostic codes, etc.

8 **COMPANY CONFIDENTIAL**

Example: an internal report that found use of the company's service increases the rate of depression in teens, an email thread between executives discussing how to handle an upcoming regulatory action by the government, etc.

9 **UNRELEASED OR SENSITIVE MARKETING**

Example: an unreleased press release in Google Docs with details about the company's upcoming product announcement, ad creative being developed in Figma with imagery of the company's unannounced product, etc.

10 **ACCOUNTING AND FINANCE DATA**

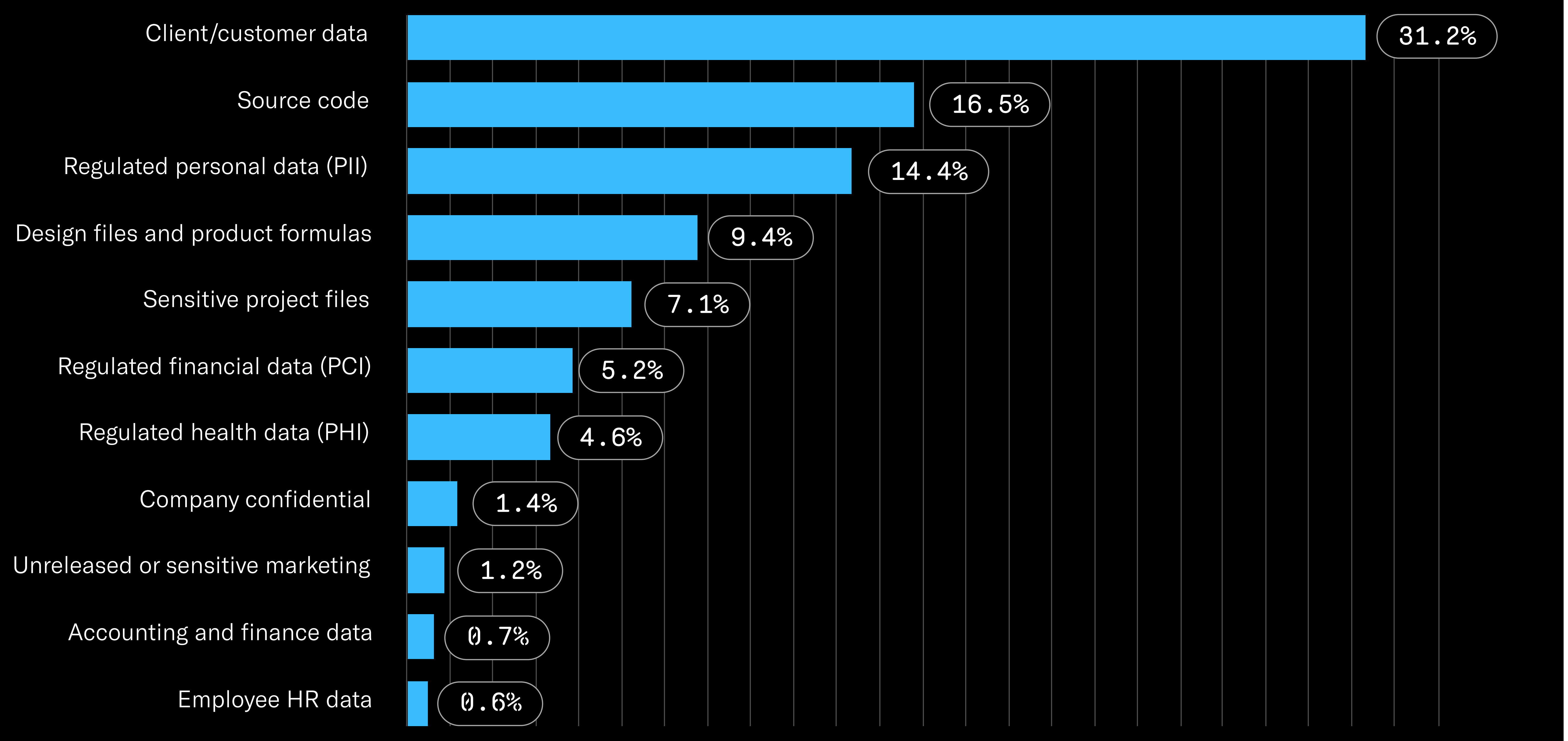
Example: a PowerPoint presentation with unreleased financials for a publicly traded company, a Google Sheet with the income statement for a company a venture capital firm is considering investing in, etc.

Client or customer information remains the most vulnerable. This category makes up 31.2% of the sensitive data that employees misappropriate. Today's enterprises have an abundance of details about their customers and documents from clients. A likely reason for this vulnerability is the failure of staff to recognize the critical nature of such data, as they might with a product design file or a healthcare record.

Source code comes in as the second highest security liability, representing 16.5% of the misappropriated data. These breaches are not limited to tech firms alone. Presently, businesses from sectors as diverse as aviation, retail, banking, and industrial production also create their own software and unique algorithms, aiming to outpace their rivals. When such proprietary code falls into the hands of competitors, it could significantly affect the company's market standing.

Top types of sensitive data employees exfiltrate

(By volume of data)



Regulated data, including personally identifiable information (PII), payment card information (PCI), and protected health information (PHI) collectively account for just 24.2% of exfiltrated data. This information, which often includes a standard alphanumeric pattern, has historically been easier to classify using software and therefore easier to protect. Our analysis finds that over 75% of exfiltrated data is harder-to-identify intellectual property (IP).

Remote, hybrid, and office work arrangements

The COVID-19 pandemic upended where knowledge work happens. Four years after the pandemic, the majority (58%) of employees in our study have a hybrid work arrangement.That means they spend some days of the week at the office and some days at home or another offsite location.

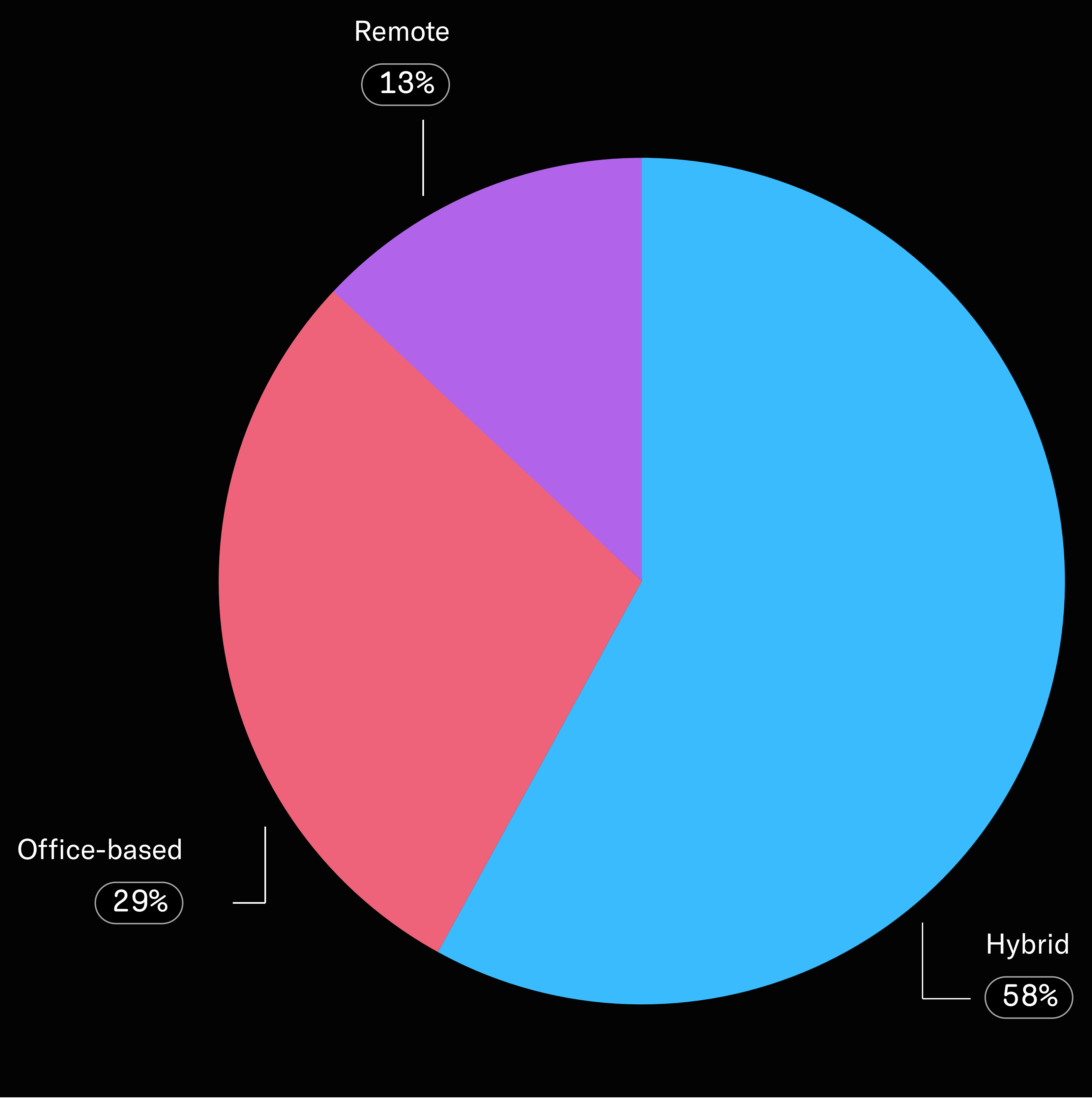
A shrinking but still sizable 13% of knowledge workers are fully remote, and another 29% are working fully from the office five days a week. The question we set out to answer is, does an employee's workplace arrangement affect how they handle sensitive information?

We analyzed the prevalence of data exfiltration incidents normalized by number of hours, which accounts how much time people spend working in a given location. Contrary to the conventional wisdom, we found that employees that are fully remote are the least likely to exfiltrate sensitive data.

On average, remote workers exfiltrate sensitive data 8.4 times for every 1 million hours worked. Employees with a fully in-office work arrangement exfiltrate data 14.9 times for every million hours, which makes them 77% more likely than their remote counterparts to exfiltrate data.

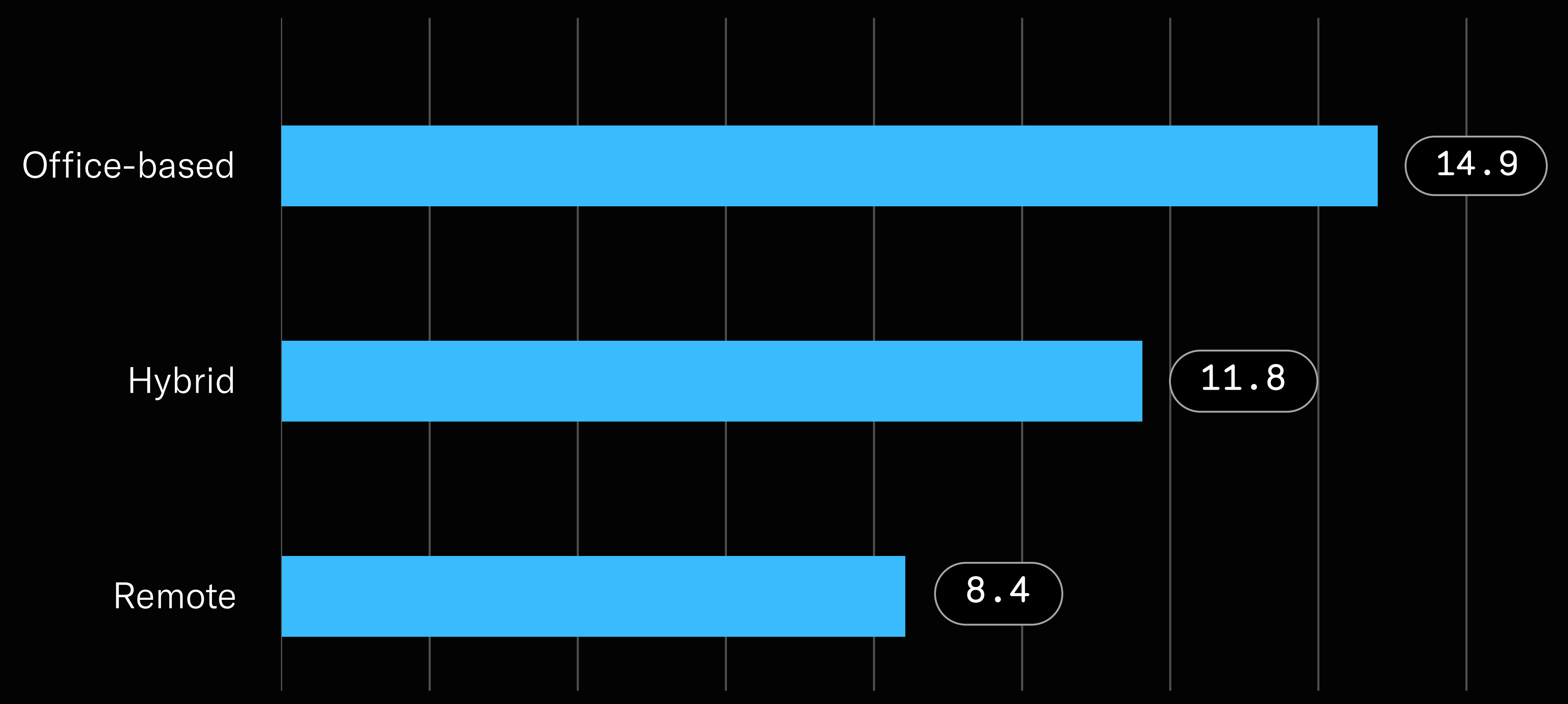
Workplace arrangements

(By percentage of employees)



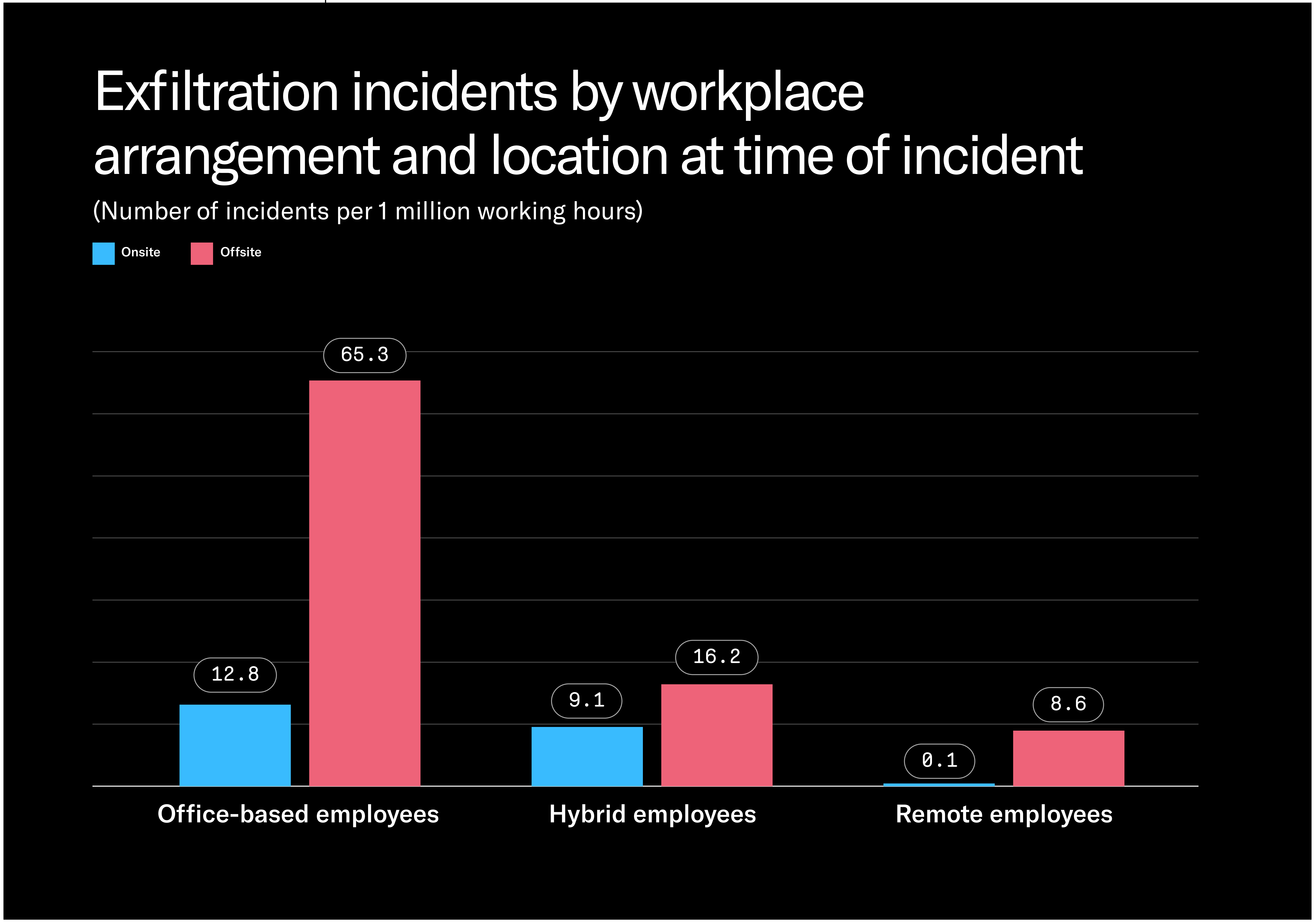
Exfiltration incidents by employee workplace arrangement

(Number of incidents per 1 million working hours)



Regardless of an employee's workplace arrangement, almost all employees in our sample did some work at the office and remotely throughout the quarter. When you look at a worker's location the exact moment they exfiltrate data, a slightly different picture emerges.

Across the board, all employees are more likely to exfiltrate sensitive data when they're offsite. But employees with fully office-based work arrangements are 510% more likely to take data when not at the office. In fact, the riskiest time for company data is when an office-based employee opens their work laptop from an offsite location. For every million hours they work offsite, a company experiences 65.3 insider incidents.



There's also a wide gap in risk depending on whether a remote employee is onsite or offsite. That's because remote employees spend a small amount of time visiting an office each quarter, and when they exfiltrate data they're extremely unlikely to do so during one of these visits. But even when they're offsite, remote employees have a lower risk of data exfiltration (8.6 incidents per million hours) than office-based employees do at the office (12.8 incidents per million hours).

The risk of employees with hybrid arrangements exfiltrating data is between that of office and remote employees on every dimension. Overall, there are 11.8 exfiltration incidents per million hours hybrid employees work, roughly in the middle of their office and remote counterparts. When they're at the office, they're less likely to exfiltrate data than fully in-office employees but when they're offsite they're also less likely to exfiltrate data during any given hour of work.

How employees exfiltrate sensitive data

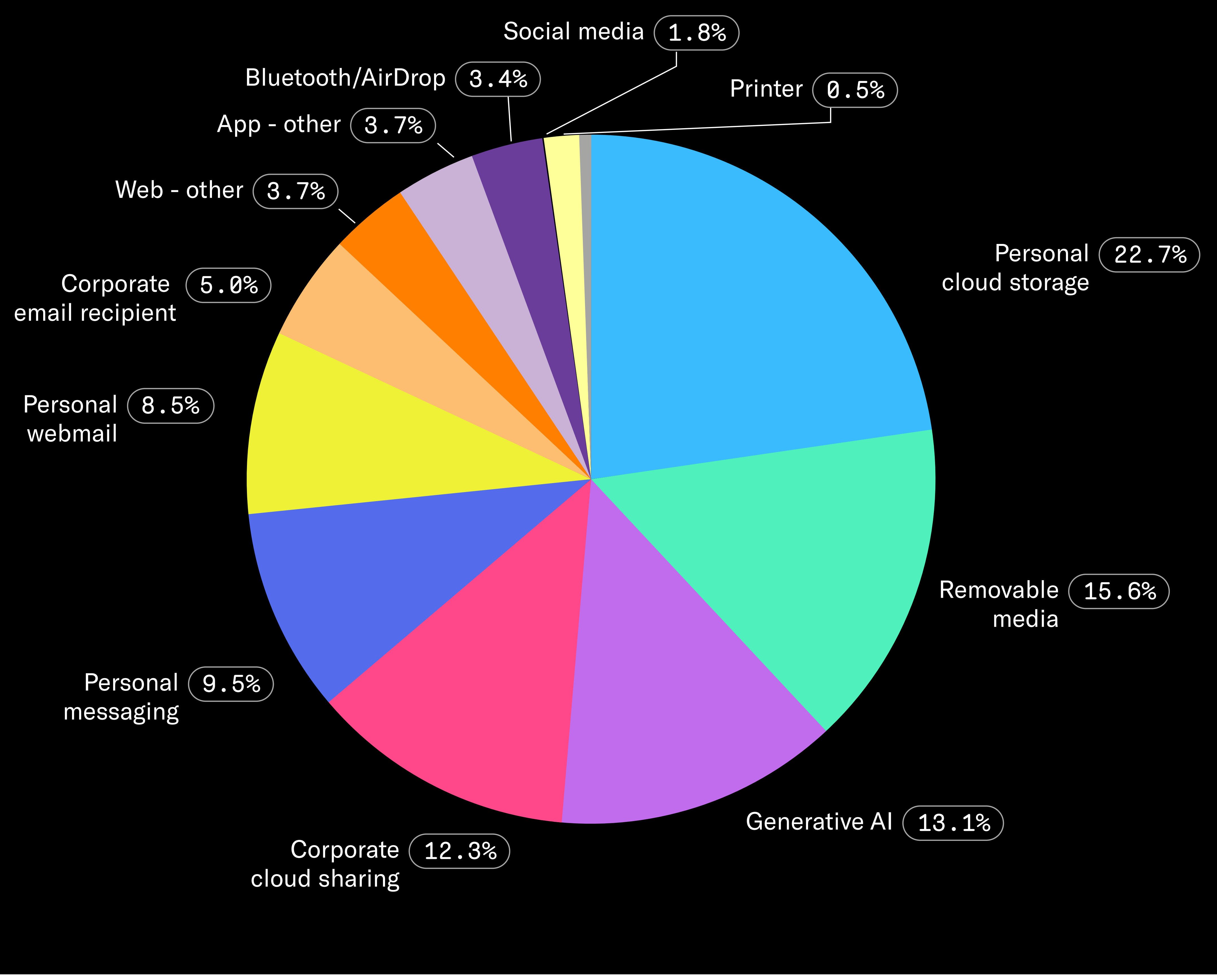
Employees take sensitive information from their companies in a variety of ways.

The top exfiltration vector is personal cloud storage, which accounts for 22.7% of all sensitive data employees take by data volume. It can be challenging for companies to detect and stop data leakage via these applications because of the widespread usage of personal accounts for the same cloud storage apps companies use, making it impractical to block access altogether.

The next most common is removable media (15.6%), which includes USB hard drives and flash drives. Cloud storage and removable media make it easy to move large amounts of data at a time, making them ideal methods for employees taking copies of all the files on their work computers with one copy and paste operation.

Destination for exfiltrated data

(By volume of data)

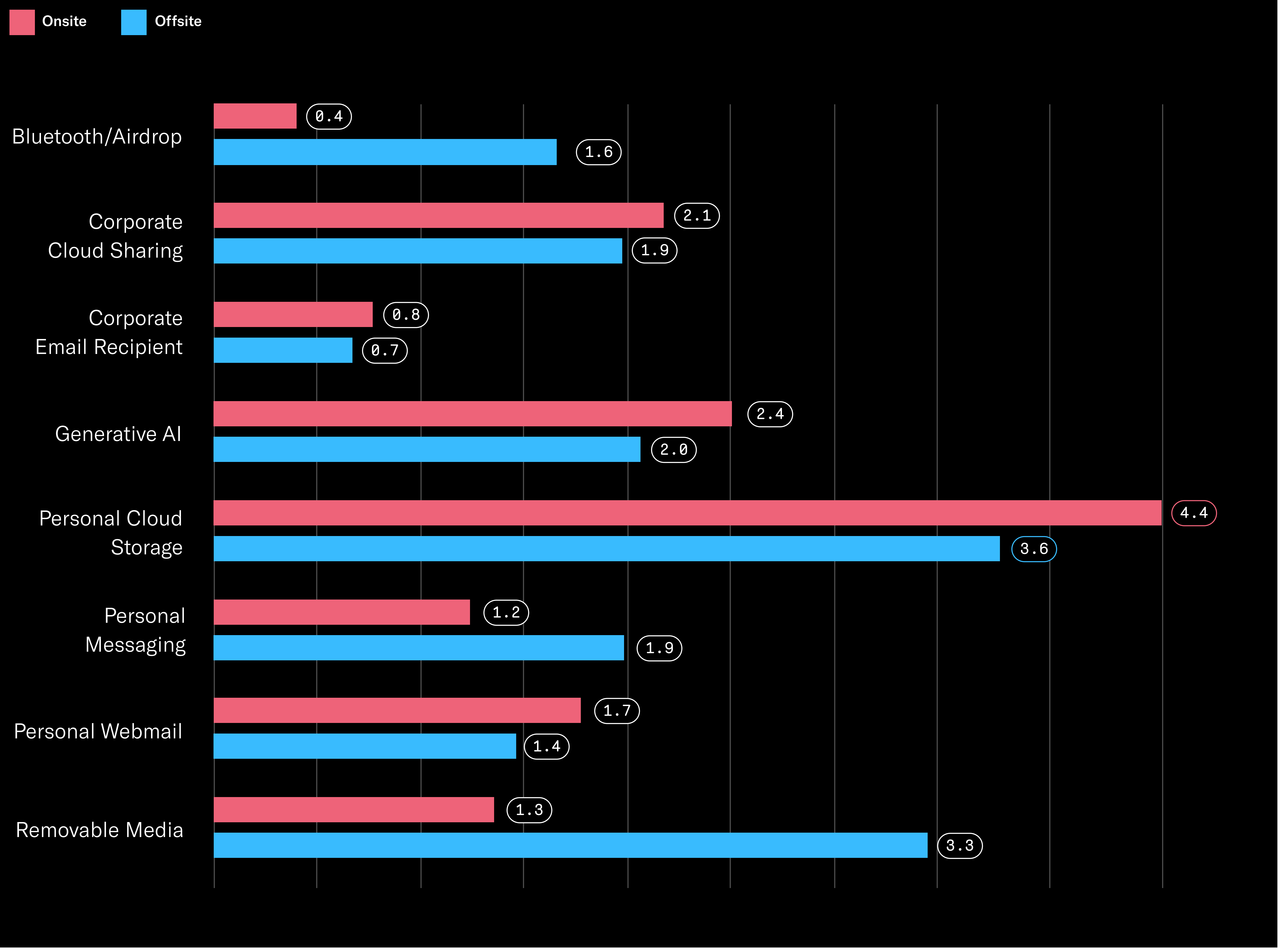


A close third is generative AI tools (13.1%) such as ChatGPT. Employees put a wide variety of sensitive company data into free generative AI accounts to accelerate their work such as summarizing strategic plans or fixing source code. But many AI products incorporate whatever you send them into their models, and can expose the substance of the information to other users outside the company.

The collaboration capabilities of many corporate cloud applications make it easy to share data outside the company, either intentionally or unintentionally, accounting for 12.3% of data exfiltration. Corporate email (5.0%) similarly provides a way to send data to your own personal email account or accidentally share something sensitive with the wrong person.

Destination of exfiltrated data by location at time of incident

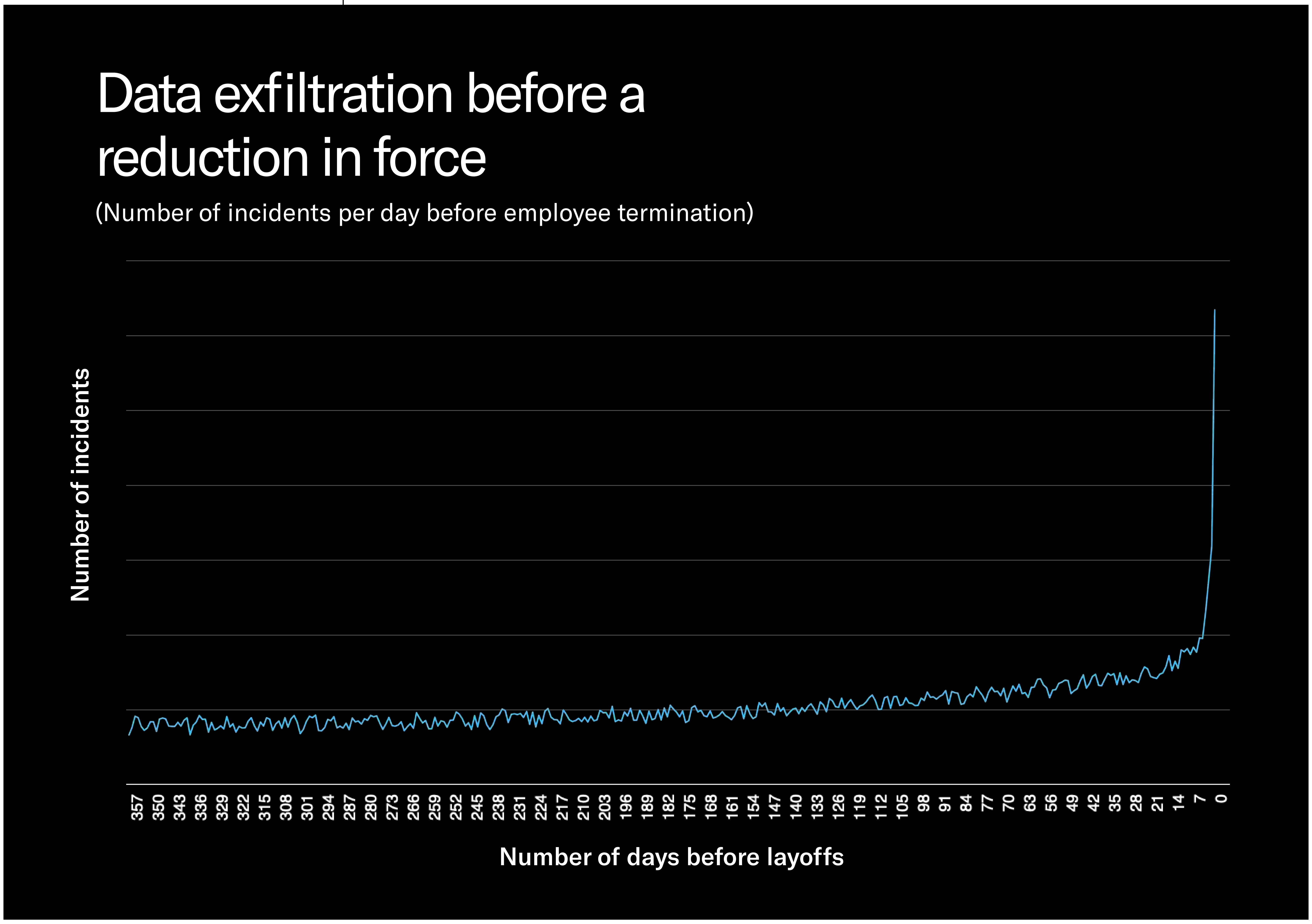
(Number of incidents per 1 million working hours)



The technology that workers use to exfiltrate company data differs depending on where they are physically located at the time of the incident. Employees are 400% more likely to use device-to-device Bluetooth file transfer technology like Apple AirDrop away from the office and they're 254% more likely to use removable storage. Perhaps this is because putting your personal laptop beside your work laptop and sending a large transfer via AirDrop would look suspicious when sitting alongside co-workers.

Anatomy of a layoff

As more companies conduct reductions in force, data security is at the forefront. We analyzed activity surrounding dozens of layoffs that occurred in 2023 to understand the implications. It's becoming more common when a company conducts a reduction in force to terminate account access for affected employees before notifying them, thereby limiting the amount of data they can take with them. But we still found a significant increase in data exfiltration before employee access is terminated. In the 24 hours before employees are notified of a layoff, there is a 720% increase in exfiltration of sensitive data compared with the baseline.


Data exfiltration before a reduction in force

(Number of incidents per day before employee termination)

The increase in data exfiltration before a layoff actually begins much earlier. We found that starting 200 days before a layoff, data exfiltration patterns begin to measurably deviate from the baseline. Three weeks before a layoff, data exfiltration reaches 150% of baseline. Whether because workers sense that they may lose their jobs or simply prepare to leave on their own is unclear, but the type of data employees exfiltrate shifts around a reduction in force.

In the seven day period prior to a layoff, employees are much more likely to take source code (348% increase over baseline), design files and product formulas (769% increase), and sensitive project files (440% increase). They are actually slightly less likely to exfiltrate regulated payment data (22% decrease) and employee HR data (16% decrease). The type of sensitive data exfiltrated ahead of a layoff appears to be concentrated in IP and work product.

Change in exfiltration by data type

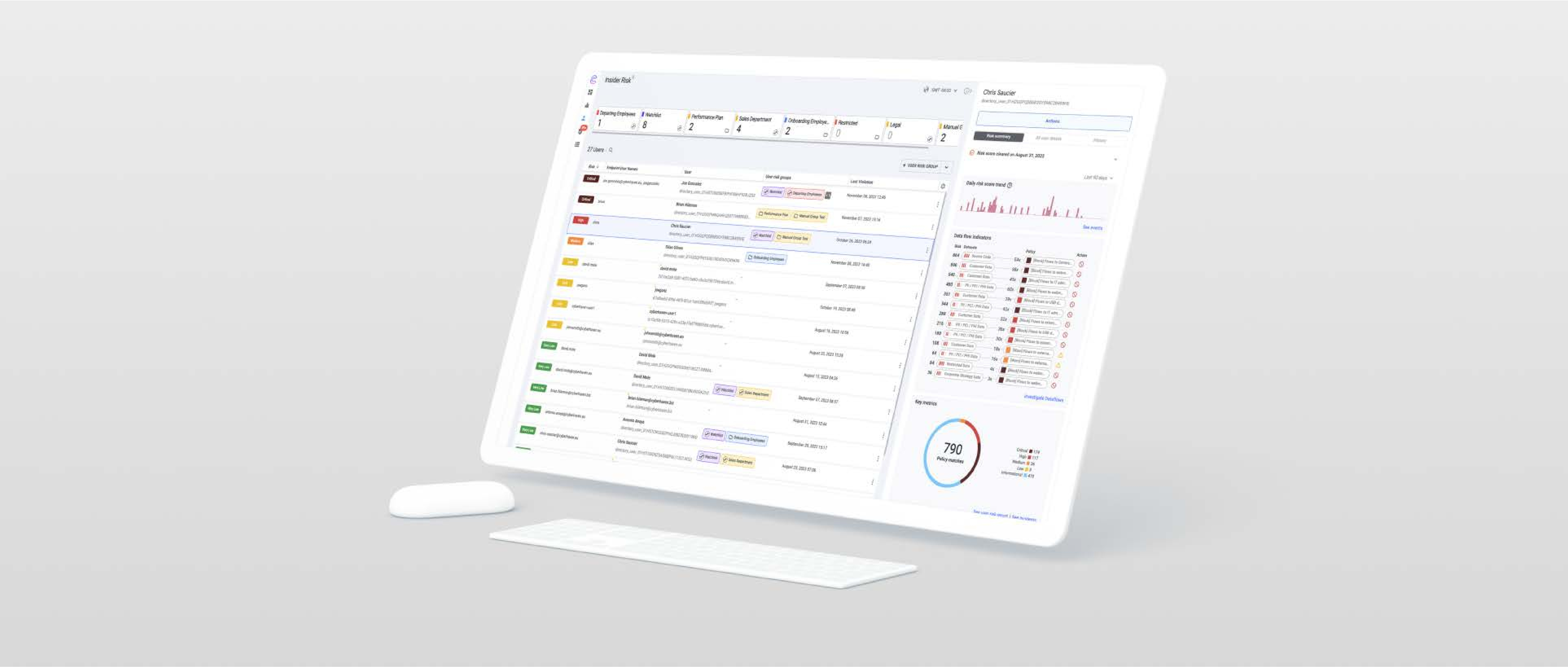
(Change in data volume in 7-days period before layoff compared to baseline)

	Change from baseline
Accounting and finance data	91% ↗
Client/customer data	8% ↗
Company confidential	211% ↗
Design files and product formulas	769% ↗
Employee HR data	-16% ↘
Regulated financial data (PCI)	-22% ↘
Regulated health data (PHI)	38% ↗
Regulated personal data (PII)	5% ↗
Sensitive project files	440% ↗
Source code	348% ↗
Unreleased or sensitive marketing	128% ↗

Detect and stop threats to your data

Get a personalized demo of how Cyberhaven can help you understand employee data usage, control risky data movement, and investigate suspicious behavior.

Request a demo today cyberhaven.com/demo



"STAYING AHEAD OF THE COMPETITION MEANS GUARDING AGAINST INSIDER THREATS. CYBERHAVEN GIVES US VISIBILITY INTO HOW DATA FLOWS WITHIN OUR COMPANY AND STOPS INSIDER THREATS IN REAL TIME."

Richard Rushing, CISO

motorola

cyberhaven

Cyberhaven is the AI-powered data security company revolutionizing how companies detect and stop the most critical insider threats to their most important data. Until now, data security products relied on manual rulesets and pre-defined policies that looked for keywords and specific user actions. Our AI technology analyzes billions of workflows to understand every piece of data within an organization, when it's at risk, and what's needed to protect it. It's like nothing that's come before and protects data like nothing else.

To learn more, visit **cyberhaven.com**